DMP:JGH/JEA
F. #2018R01373

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

| | |
|---|---|
| IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS THE HOME OFFICE INSIDE OF 20-56 42ND STREET, QUEENS, NEW YORK 11105, AND THE HEWLETT PACKARD PAVILION DESKTOP COMPUTER FOUND THEREIN | APPLICATION FOR A SEARCH WARRANT<br><br>20-M-265 |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, JOSEPH DORNBIERER, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as the home office inside of 20-56 42nd Street, Queens, New York 11105 (the "SUBJECT PREMISES"), and the Hewlett Packard Pavilion desktop computer found therein, as further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been a Special Agent with HSI for over 3 years, and a federal law enforcement officer for more than 15 years, during which I have been responsible for conducting and assisting investigations into, among other things, criminal

activity involving computers such as hacking, computer network intrusions, money laundering, check fraud, bank fraud, credit card fraud, and identity theft. I am currently assigned to HSI Cyber Division's Cyber Intrusion and Fraud Group. During my time with HSI, I have conducted or participated in surveillance, the execution of search warrants, debriefings of informants, and the review of other evidence. Through my training, education, and experience, I have become familiar with the manner in which people use computers to commit crimes and the law enforcement techniques that can be utilized to investigate and disrupt such activity. Moreover, in the course of my investigations and other cases on which I have worked, I have gained experience executing search warrants for both physical premises and electronic evidence and data, including the content and other data associated with cellphones, email, messenger, financial, and digital-marketplace accounts.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this Affidavit, I respectfully submit that there is probable cause to believe that there presently is located in the SUBJECT PREMISES certain items and property, which are more fully set forth in Attachment B, which constitute evidence, fruits and instrumentalities of violations of, *inter alia*: 18 U.S.C. §§ 1343, 1344 and 1349 (bank fraud, wire fraud and conspiracy to commit the same); 18 U.S.C. § 1028 (fraud in connection with identity documents and conspiracy to commit the same); 18 U.S.C. §§ 1028A and 371 (aggravated identity theft and conspiracy to commit the same); 18 U.S.C. § 1644 (fraudulent use of credit cards); and 18 U.S.C. §§ 1956 and 1957 (money laundering and conspiracy to commit the same) (collectively, the "Subject Offenses").

## DESCRIPTION OF SUBJECT PREMISES

5. The SUBJECT PREMISES to be searched is the first floor home office inside of the private house located at 20-56 42nd Street, Queens, New York 11105 (the "42nd Street Residence"), and to include the Hewlett Packard Pavilion desktop computer (the "HP Desktop Computer"). Upon entering the side door entrance of the 20-56 42nd Street residence, the SUBJECT PREMISES to be searched is located to the left on the first floor of the house.

## PROBABLE CAUSE

I. Background

6. The United States Attorney's Office for the Eastern District of New York, HSI, the Internal Revenue Service – Criminal Investigation ("IRS–CI"), the New York City Police Department and the New York County District Attorney's Office, are investigating a years-long conspiracy perpetrated by ABED AHMAD ("ABED"), ALAA AHMAD ("ALAA"), CLAUDIA AYOUB, MOUSTAFA AYOUB and CONSTANTINE VASES ("VASES"), and others. The investigation has revealed that from in or about November 2012 through in or about June 2017 (the "Charged Period"), these coconspirators conspired with each other and others to defraud JPMorgan Chase & Co. ("JPMC") and its customers by misappropriating more than $7.6 million from numerous victim bank accounts held at JPMC (the "JPMC Victim Accounts").

7. On February 3, 2020, this Court signed a Criminal Complaint (Mag. No. 20-106, hereinafter the "Complaint") and issued arrest warrants for ABED, ALAA, CLAUDIA AYOUB, MOUSTAFA AYOUB and VASES (collectively, "the Defendants") for conspiring

together and with others to commit bank fraud and money laundering. The Complaint is attached hereto as Exhibit 1 and hereby incorporated by reference.

8. On February 4, 2020, the Defendants were arrested and charged pursuant to the Complaint. Both MOUSTAFA AYOUB and CLAUDIA AYOUB[1] were arrested at the SUBJECT PREMISES address. On March 18, 2020, a grand jury in the Eastern District of New York returned a three-count indictment (the "Indictment") charging MOUSTAFA AYOUB with one count of bank fraud conspiracy, one count of money laundering conspiracy and one count of aggravated identity theft. See Crim. No. 20-142 (ENV). The Indictment includes a forfeiture allegation against the 42nd Street Residence based upon the property's use in facilitating the charged money laundering offense. The United States is continuing to investigate the involvement of additional coconspirators in the Subject Offenses, as well as multiple additional acts of, *inter alia*, aggravated identity theft and fraudulent use of credit cards committed by MOUSTAFA AYOUB and others.

9. As detailed in the Complaint, the Defendants conspired with each other and others to misappropriate funds from the JPMC Victim Accounts in two central ways. The first method was to transfer money directly from the JPMC Victim Accounts that were accessed by ABED and ALAA while they were working at JPMC. These initial transfers were made predominantly through fraudulent checks, online and wire transfers into numerous "First Pass" bank accounts held at various financial institutions.[2] The majority of these First

---

[1] The Complaint indicated Claudia Ayoub is Moustafa Ayoub's girlfriend. The investigation has since revealed that Claudia and Moustafa Ayoub were married in Mexico approximately ten years ago, though the marriage may not be legally valid.

[2] "First Pass" refers to the initial transfer of funds from the JPMC Victim

Pass financial accounts were held in the names of (1) Naim Ayoub, who is referred to in the Complaint as Individual-1 and who left the United States in approximately July 2011 and has not returned since, and (2) Robert Elsaleh, who is referred to in the Complaint as Individual-2 and who left the United States in approximately September 2014 and has not returned since. In reality, however, and as set forth in detail in the Complaint, these First Pass financial accounts were controlled and operated by the Defendants and their coconspirators. The Defendants and their coconspirators then used these First Pass accounts to transfer the stolen funds and launder them through a second layer of personal and business bank accounts used and controlled by the Defendants and other members of the conspiracy, including into the accounts of shell companies they created and controlled. The Defendants and their coconspirators then further laundered the stolen funds by transferring them to other financial accounts that they controlled. Using this method, the Defendants misappropriated and laundered millions of dollars from JPMC Victim Accounts.

10. The other primary method the Defendants used to misappropriate funds from the JPMC Victim Accounts involved transferring the funds from JPMC Victim Accounts to make payments to a series of credit card accounts controlled and operated by the Defendants and their coconspirators. The Defendants used credit cards, again in the names of Naim Ayoub and Robert Elsaleh, to charge sales by the shell companies they controlled, principally using point of sale ("POS") terminals obtained by VASES. They then transferred funds from the JPMC Victim Accounts to pay these charges, which had the effect of transferring the funds

---

Accounts into a set of financial accounts controlled and managed by members of the conspiracy.

from the JPMC Victim Accounts to the shell companies controlled by the Defendants. The Defendants also transferred personal credit card balances to the credit cards in the names of Naim Ayoub and Robert Elsaleh, and then used funds from the JPMC Victim Accounts to pay off the credit card balances.

11. The investigation, including a review of bank and credit card records, has revealed that the following entities and/or financial accounts held in their names, were used in furtherance of the bank fraud and money laundering conspiracies charged in the Complaint, as well as fraud in connection with identity documents and credit card fraud: Freeform International, Inc.; Blackstone Capital Group, LLC; M&H Sportswear, Inc.; Clothing Zone; Global Network Marketing Solutions, Inc.; Swap Real Estate, LLC; Silvermist, Inc.; Everest, Inc.; Astoria Food Mart, Inc., a/k/a Cedar, a/k/a Al Nour; Milkway Knitwear, Inc.; Melville Parkway, Inc.; and Woodbury Port, Inc.

## II. MOUSTAFA AYOUB and the SUBJECT PREMISES

12. The SUBJECT PREMISES is located inside the 42nd Street Residence, the current residence of MOUSTAFA AYOUB,[3] CLAUDIA AYOUB and their children. As set forth in the Complaint, the 42nd Street Residence containing the SUBJECT PREMISES was used by MOUSTAFA AYOUB and CLAUDIA AYOUB in furtherance of the bank fraud and money laundering conspiracies to, among other things, operate numerous bank and credit card accounts used to receive and/or launder funds stolen from JPMC Victim Accounts.

---

[3] MOUSTAFA AYOUB is currently detained at the Metropolitan Detention Center in Brooklyn pending trial on the charges contained in the Indictment.

13. For example, the investigation has revealed that MOUSTAFA AYOUB used the 42nd Street Residence as the address for multiple financial accounts that he opened and operated in the name of his adult daughter, Manife Ayoub.[4] Indeed, records and other evidence show that MOUSTAFA AYOUB repeatedly used Manife Ayoub's name and personally identifiable information ("PII"), including her social security number, to open and operate these financial accounts while Manife Ayoub was living outside the United States, all without her knowledge or consent. MOUSTAFA AYOUB operated these accounts in Manife Ayoub's name, including multiple bank accounts, in furtherance of the conspiracies charged in the Indictment.

14. Several of the bank accounts that MOUSTAFA AYOUB unlawfully opened in Manife Ayoub's name using the 42nd Street Residence address were used to receive and/or launder hundreds of thousands of dollars of stolen JPMC victim funds. For example, records show that in or about January 2015, while Manife Ayoub was living outside the United States, MOUSTAFA AYOUB used the internet to apply for and open a checking account at Citibank in the name of Manife Ayoub ending in the numbers 0285 (the "Manife Ayoub 0285 Account"). The online application for the Manife Ayoub 0285 Account shows that MOUSTAFA AYOUB used Manife Ayoub's social security number and date of birth to open the account, and that he listed the 42nd Street Residence as the account address. The investigation has revealed that the Manife Ayoub 0285 Account was used by MOUSTAFA AYOUB to receive tens of thousands of dollars of unlawfully misappropriated funds from JPMC Victim Accounts as part of the bank fraud conspiracy charged in the Indictment.

---

[4] Manife Ayoub is identified as "Jane Doe #1" in Count Three of the Indictment.

15. Furthermore, bank records, including phone calls recorded by the financial institutions as part of their regular course of business, show that on multiple occasions during the Charged Period, MOUSTAFA AYOUB used the telephone number 718-606-1518 to call the companies pretending to be Manife Ayoub. During these calls, MOUSTAFA AYOUB used Manife Ayoub's PII to operate one or more credit card accounts that MOUSTAFA AYOUB opened in her name without her knowledge or consent.

16. Records further show that 718-606-1518 is a telephone registered to the 42nd Street Residence in the name of "Claudia Ayoub." The email account associated with the telephone number is "clothingzone@aol.com," an email address used and controlled by MOUSTAFA AYOUB.

17. Additionally, a review of bank and Internet Protocol ("IP") records shows that the IP address associated with the 42nd Street Residence was registered in the name of CLAUDIA AYOUB and was used to log in to multiple financial accounts in the name of, among others, Manife Ayoub, in furtherance of the Subject Offenses. For example, IP records show that from approximately May through December 2016, the IP address associated with the SUBJECT PREMISES address was used numerous times to log in to a Capital One business credit card account in the name of Manife Ayoub ending in 5539 (the "Manife Ayoub Capital One 5539 Account"). The Manife Ayoub Capital One 5539 Account was opened in Manife Ayoub's name without her knowledge or consent in or about December 2015, when Manife Ayoub was living outside the United States, using the 42nd Street Residence as the account address. The business associated with the Manife Ayoub Capital One 5539 Account is listed as Woodbury Port, Inc. As detailed in the Complaint, Woodbury Port, Inc. was a shell company created using Manife Ayoub's name without her knowledge or consent while

she was outside the United States. MOUSTAFA AYOUB and other coconspirators used Woodbury Port and bank accounts in its name to steal funds from JPMC Victim Accounts.

18. Furthermore, as set forth above, both MOUSTAFA AYOUB and CLAUDIA AYOUB were arrested on February 4, 2020 at the 42nd Street Residence. While conducting a security sweep inside the 42nd Street Residence, including the SUBJECT PREMISES, a law enforcement officer observed, in plain view atop the desk inside the SUBJECT PREMISES, two stacks of what appeared to be credit and/or bank cards, with each stack appearing to contain approximately twenty to twenty-five cards.

19. The government has also received information from a confidential source ("CS-1")[5] that the SUBJECT PREMISES contains evidence of the Subject Offenses. Specifically, CS-1 has informed law enforcement that the HP Pavilion Computer located atop

5 [redacted]

the desk inside the SUBJECT PREMISES is a computer that MOUSTAFA AYOUB has used for approximately the last 5 years. CS-1 has further informed law enforcement that the computer contains a copy of Manife Ayoub's social security number, as well as a copy of Manife Ayoub's New York State identification card.

20. CS-1 has further informed law enforcement that atop the desk inside the SUBJECT PREMISES is a pad of paper containing the handwritten account passwords and security questions for numerous financial accounts in the name of multiple individuals, including CS-1. CS-1, who is familiar with MOUSTAFA AYOUB's handwriting, has informed law enforcement that the handwriting on the pad is MOUSTAFA AYOUB's handwriting. CS-1 has also informed law enforcement that the desk inside the SUBJECT PREMISES contains a folder with documents in the names of MOUSTAFA AYOUB's parents. Bank records show that in or about May 2014, two financial accounts – one at E-Trade and one at TD Ameritrade – were opened in the name of MOUSTAFA AYOUB's father, Sobhi Ayoub. Bank records further show that the address associated with these two accounts was MOUSTAFA AYOUB's and CLAUDIA AYOUB's rental apartment on 29th Street in Queens, New York, which, as set forth in the Complaint, MOUSTAFA AYOUB continued to pay rent for after he and CLAUDIA AYOUB moved to the 42nd Street Residence. Also as set forth in the Complaint, the 29th Street residence, just like the 42nd Street Residence, was used as an address for numerous fraudulently operated financial accounts used to commit the charged bank fraud and money laundering conspiracies.

21. Bank records also show that in or about April 2014, a TD Ameritrade account was opened in the name of MOUSTAFA AYOUB's mother, Manife S. Ayoub, and that the address associated with the account was the 29th Street residence.

22. At the time these three accounts were opened in the names of MOUSTAFA AYOUB's parents, they were living outside of the United States.

23. Based on my training and experience – including my participation in this investigation – I have learned that individuals who engage in fraudulent conduct such as the Subject Offenses as described herein often keep physical evidence, fruits, and instrumentalities of their crimes inside their home offices and stored and saved within computers inside those home offices.

24. Additionally, I know from my knowledge, training and experience that such evidence, fruits and instrumentalities are often stored in locked containers, safes, secret compartments, closets, drawers, above or below ceiling and floor tiles, behind false walls and, when digital in nature, inside locked or lockable electronic devices (e.g., computers and smart telephones) and in other places intended to avoid detection by other people, including law enforcement.

25. Accordingly, and based on all of the above, I submit that there is probable cause to believe that the SUBJECT PREMISES, including the HP Pavilion Computer found therein, will contain evidence, fruits and instrumentalities of the Subject Offenses.

## TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

(a) IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so

that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

(b) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

(c) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

**COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

27. As described above and in Attachment B, this application seeks permission to search for certain documents and records that might be found inside the SUBJECT PREMISES, including on the HP Pavilion Computer therein, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

(a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

(b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

(c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

(d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES, including the HP Pavilion Computer, because:

(a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

(b) As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional

information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information

within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

(c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

(d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

(e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

30. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media, such as the HP Pavilion Computer, often requires the seizure of the physical storage

media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

(a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

(b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-

site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

(c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the law enforcement officers executing this warrant to image, or otherwise copy, storage media that reasonably appear to contain some or all of the evidence described in the warrant, including the HP Pavilion Computer, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. In the event that the law enforcement officers executing the warrant are unable to image, or otherwise copy, storage media encompassed by the warrant on-site, the warrant I am applying for would permit law enforcement officers executing the warrant to seize such storage media for a reasonable amount of time, in order to complete the imaging, or other copying, process at an off-site location.

32. Because several people share the SUBJECT PREMISES, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those

computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

## CONCLUSION

WHEREFORE, your deponent respectfully requests that a warrant be issued, pursuant to Federal Rule of Criminal Procedure 41, to search the SUBJECT PREMISES, which is the first floor home office inside the 42nd Street Residence, as further described in Attachment A, and to seize those items set forth in Attachment B, including the HP Pavilion Computer, that may constitute evidence, fruits and instrumentalities of violations of the Subject Offenses.

JOSEPH DORNBIERER
Special Agent, HSI

Sworn to before me this
24th day of March, 2020

THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

**ATTACHMENT A**

*Property to be Searched*

The property to be searched is the first floor home office inside of the private residence located at 20-56 42nd Street in Queens, New York 11105 (the "SUBJECT PREMISES"), to include the Hewlett Packard Pavilion desktop computer. Upon entering the side door entrance of the 20-56 42nd Street residence, the SUBJECT PREMISES to be searched is located to the left on the first floor of the house.

**ATTACHMENT B**

*Property to be Seized*

1. For the period from in or about November 2012 through in or about December 2017, all items, including records and information, that constitute evidence, fruits and instrumentalities relating to violations of 18 U.S.C. §§ 1343, 1344, 1349 (bank fraud, wire fraud and conspiracy to commit the same); 18 U.S.C. § 1028 (fraud in connection with identity documents and conspiracy to commit the same); 18 U.S.C. §§ 1028A and 371 (aggravated identity theft and conspiracy to commit the same); 18 U.S.C. § 1644 (fraudulent use of credit cards); and 18 U.S.C. §§ 1956, 1957 (money laundering and conspiracy to commit the same) (collectively, the "Subject Offenses"), including but not limited to:

(a) Any and all records, including but not limited to, identifying documents, credit card & bank statements, applications to financial institutions, including banks and credit card companies, correspondence to/from financial institutions, bookkeeping records, including inventory records and accounting journals, records of wire and/or online transfers, deposit items, checks, withdrawal items, banking financial receipts, income tax returns, correspondences and applications to/from credit card/merchant processors, company bills, records identifying ownership of entities, emails, invoices, handwritten notes, and all account information, including login names, account passwords, security questions/answers, related to the following individuals and entities:

1. Moustafa Ayoub;
2. Claudia Ayoub;
3. Manife Ayoub;
4. Sobhi Ayoub;
5. Manife S. Ayoub;
6. Mohamed Ayoub;
7. Naim Ayoub;
8. Robert Elsaleh;
9. Constantine Vases;
10. Abed Ahmad;
11. Alaa Ahmad;
12. Freeform International, Inc.;
13. Blackstone Capital Group, LLC;
14. M&H Sportswear, Inc.;
15. Global Network Marketing Solutions, Inc.;
16. Swap Real Estate, LLC;
17. Silvermist, Inc.;
18. Everest, Inc.;
19. Clothing Zone;
20. Astoria Food Mart, Inc., a/k/a Cedar, a/k/a Al Nour
21. Milkway Knitwear, Inc.;

22. Melville Parkway, Inc.; and
23. Woodbury Port, Inc.

(b) Any and all credit cards, debit cards, bank cards and store membership cards;

(c) All documents, including bills, related to cell phones held in the names of Moustafa Ayoub and Naim Ayoub;

(d) Point of sale terminals;

(e) Computers or storage media used as a means to commit the Subject Offenses, including the Hewlett Packard Pavilion desktop computer;

(f) For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

i. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of COMPUTER access, use, and events relating to crime under investigation and to the COMPUTER user;

v. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

vi. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

viii. evidence of the times the COMPUTER was used;

ix. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

x. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

xi. records of or information about Internet Protocol addresses used by the COMPUTER;

xii. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

xiii. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.